



DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G3/5/7
400 ARMY PENTAGON
WASHINGTON DC 20310-0400

DAMO-FMS

23 October 2013

MEMORANDUM FOR All personnel Assigned/Attached to the Army Force Management School (AFMS)

SUBJECT: AFMS Policy Letter #2 – Army Force Management School Essential Elements of Friendly Information (EEFI) Operational Security Program

1. References:

a. ALARACT OPSEC Message, 221224Z May 06, subject: Guidance on the Proper Use of Hardware and Software.

b. AR 530-1, Operations Security, 19 Apr 07.

c. AR 380-5, DA Information Security Program, 29 Sep 00.

2. With the advent of the computer, the picture cell phone, the internet and the frequent substitution of face to face meetings with email and electronic collaborations, the potential for inadvertent disclosure of sensitive information concerning our operations has greatly increased.

3. To more clearly define the information that we must protect from our adversaries, we have developed a number of Essential Elements of Friendly Information (EEFI) for the school:

- a. Location, schedule, and security arrangements for senior leaders and visiting VIPs.
- b. Security, disposition, and location of information network.
- c. Assets/VIPs deployed and the purpose, itinerary, and destination of the deployment.
- d. Location of mission essential vulnerable areas, high risk targets, and the measures employed to secure them.
- e. Measures to mitigate force protection vulnerabilities.
- f. Force Protection Condition Measures.
- g. Security measures planned or implemented for high visibility, high personnel concentration events.

4. EEFI are critical aspects of a friendly operation that if known by our adversaries, could compromise, lead to failure, or limit success of that operation and therefore must be protected from enemy detection.

DAMO-FMS

SUBJECT: AFMS Policy Letter #2 – Army Force Management School Essential Elements of Friendly Information (EEFI) Operational Security Program

5. Effective immediately, information pertaining to our EEFI will be treated at a minimum as "For Official Use Only", meaning that such information will not be transmitted by non-secure means:

a. Data determined to be sensitive but unclassified will at a minimum be encrypted using CAC/PKI.

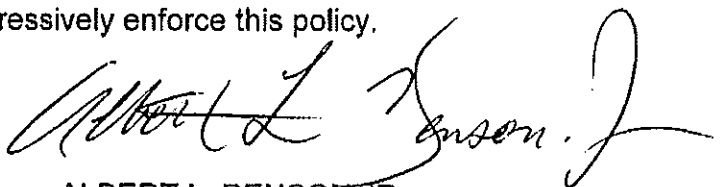
b. Classified information (e.g., CONFIDENTIAL, SECRET, etc.) will be transmitted over a network with a minimum security classification of SECRET (e.g., SIPERNET).

c. Unclassified critical and sensitive operational traffic over a secure network. For the purpose of this memorandum, unclassified critical and sensitive operational traffic will include but not be limited to correspondence containing General Officer and Senior Executive Service (SES) overseas travel schedules and all deployed and deploying troop information.

d. All lessons learned on emerging Tactic, Techniques, and Procedures (TTP) related to Operation Iraqi Freedom (OIF), Operation Noble Eagle (ONE), and Operations Enduring Freedom (OEF) will be transmitted over a network with minimum security classification SECRET.

e. If, after reviewing the references and consulting with your security manager, it remains unclear whether the data is appropriate for an unclassified network, restrict transmission to a secure network until authoritative guidance is received. Even where CAC/PKI is used, the NIPRNET is not considered a "secure" network.

6. I expect all individuals at all levels to aggressively enforce this policy.

A handwritten signature in black ink, appearing to read "Albert L. Benson Jr.", with a stylized flourish at the end.

ALBERT L. BENSON JR.
Lieutenant Colonel, LG
Deputy Commandant, AFMS

Encl

Enclosure 1

Army Force Management School EEFI

- a. What are the vulnerabilities and security measures of AFMS information Systems?
- b. What are the sensitive non-public major AFMS events, times, locations, attendees, and security plans?
- c. What are the Itineraries of general officers (GOs), senior executive service (SES), very important persons (VIPs) and distinguished visitors (DVs)?
- d. What are the AFMS critical assets, mission essential vulnerable areas (MEVAS), high-risk targets (HRTs), and what are the security measures and plans to protect them?
- e. What are the identification and security measures applied against AFMS as a High Risk Target on Ft Belvoir?
- f. What are the plans for initiation of contingency operations or deployment of key personnel affecting AFMS?
- g. What are the shortfalls in training and/or operations (i.e. print or electronic) due to funding?
- h. Which measures does AFMS use to reconcile or mitigate force protection vulnerabilities such as specific FPCON measures?
- i. What are the AFMS information sources that provide insights on Doctrine, Organization, Training Material, Leadership and Education, Personnel and Facilities (DOTMLPF) developments, lessons learned or emerging tactics, techniques, and procedures (TTPs) related to current or future operations.